Synopsis

On

“Student’s Lab Authorization Using Fingerprint Biometric ”

Submitted for partial fulfilment of the diploma in

Computer Technology

By

Name of projectee’s

- **Omprakash Sahu**
- **Om Ainchwar**
- **Ameya Tatkundwar**
- **Ayush Jagnade**
- **Akshay Gedam**
- **Prasad Guddewar**
- **Sahili Marwade**

Under the Guidance of

Prof . S.K.Kharkate

Department of Computer Technology

GOVERNMENT POLYTECHNIC, BRAMHAPURI
DIST.CHANDRAPUR

Index

Sr.no	Contents	Page no.
1.	Chapter 1 – Problem Defination and Abstract	
2.	Chapter 2 – Introduction	
3.	Chapter 3 – Design (Data Flow and Structure Flow / ER Diagram)	
4.	Chapter 4 – Implementation Details	
5.	Chapter 5 – Hardware & Software Requirements	
6.	Conclusions	
8.	References	

Chapter 1 - Problem definition and Abstract

1.1 Problem Definition :

The problem at hand is to design and implement a "Students Lab Authorization System Using Fingerprint Biometric" to ensure secure and convenient access to laboratory facilities for authorized students within an educational institution.

Background:

In many educational institutions, especially those with valuable equipment and sensitive experiments, access to laboratories needs to be tightly controlled to maintain security and safety. Traditional access control methods such as keys or access cards can be susceptible to issues like loss, theft, or unauthorized duplication. To address these challenges, the implementation of a fingerprint biometric system is proposed.

Problem Statement:

The primary problem is the lack of a reliable and efficient access control system for laboratories within the educational institution, leading to concerns related to security, accountability, and convenience. Key issues to be addressed include:

1. Unauthorized Access: The current access control methods, such as keys and access cards, are prone to unauthorized access. Students may lend their cards to others or lose them, compromising the security of the laboratories.

2. Security Concerns: Ensuring the security of sensitive laboratory equipment, experiments, and intellectual property is paramount. Unauthorized access poses a significant security risk.

3. Accountability: There is a lack of an efficient system for tracking who enters and exits the laboratories. In the event of an incident, it is challenging to identify the individuals involved.

4. Convenience: Students and authorized personnel often face inconvenience with traditional access methods, such as carrying access cards, which can be lost or forgotten. An efficient and user-friendly access system is needed.

1.2 Abstract :

In educational institutions where valuable equipment and sensitive experiments are housed, ensuring secure and convenient access to laboratory facilities for authorized students is a paramount concern. This paper delves into the multifaceted challenges associated with conventional access control methods, such as physical keys and access cards, which are susceptible to unauthorized access, security breaches, and accountability lapses. In response to these pressing issues, we propose the design and implementation of a cutting-edge "Students Lab Authorization System Using Fingerprint Biometric."

The proposed system addresses a quartet of vital aspects:

1.Security Enhancement: Unauthorized access and breaches in laboratory security pose significant risks. Traditional access methods are prone to vulnerabilities. The fingerprint biometric system ensures robust security by authenticating authorized users through their unique fingerprints, thus eliminating the threats associated with keys and access cards.

2. Accountability and Monitoring: Accurate monitoring of laboratory access is essential for maintaining accountability. Traditional systems often fall short in providing detailed records of who enters and exits laboratories. The proposed system offers real-time monitoring and comprehensive logging capabilities, providing administrators with the means to track access and respond effectively to incidents.

3. Convenience and User Experience: Conventional access methods, such as access cards, can be inconvenient for students and authorized personnel, often requiring them to carry additional items and navigate potentially faulty or lost cards. The fingerprint biometric system enhances convenience by offering a user-friendly, seamless experience. Users simply need to place their fingertip on the scanner, eliminating the need for physical tokens.

4. Mitigating Unauthorized Intrusion: Unauthorized access not only jeopardizes the safety of valuable laboratory equipment but also poses a substantial risk to the institution as a whole. The implementation of fingerprint biometrics serves as a robust defense against unauthorized intrusion, bolstering the overall security posture of the educational institution.

By adopting this cutting-edge solution, educational institutions can leap forward in safeguarding valuable resources and streamlining access within the educational environment, heralding a new era of laboratory security and management.

Chapter 2 – Introduction

2.1 Introduction:

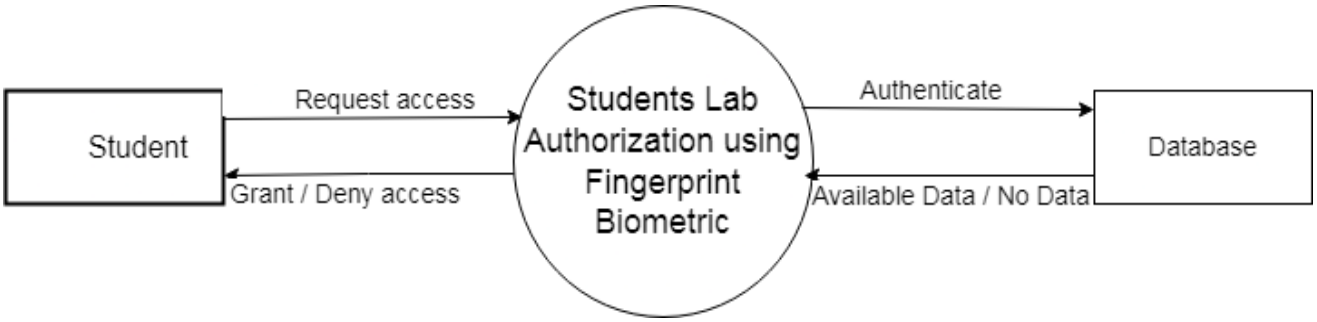
In educational institutions across the globe, laboratories stand as the hubs of ingenuity, experimentation, and experiential learning. These dynamic environments are home to an array of invaluable equipment and serve as the backdrop for the most sensitive and groundbreaking experiments. Consequently, the imperative for stringent access control measures cannot be overstated. While conventional access methods, such as physical keys or access cards, have long been the standard, they carry inherent vulnerabilities. These conventional methods are susceptible to unauthorized access, security breaches, and the challenges of maintaining meticulous accountability.

Acknowledging the inadequacies of traditional access systems, this paper introduces a pioneering concept: " Student Lab Authorization Using Fingerprint Biometric." By harnessing the formidable capabilities of biometric authentication, particularly fingerprint recognition, this system presents a transformative paradigm for laboratory access control within educational institutions. It represents an innovative solution designed to not only elevate security and accountability to unprecedented levels but also to simplify the user experience dramatically. In doing so, it heralds the advent of a new era characterized by heightened efficiency and unswerving reliability in the realm of educational laboratory management.

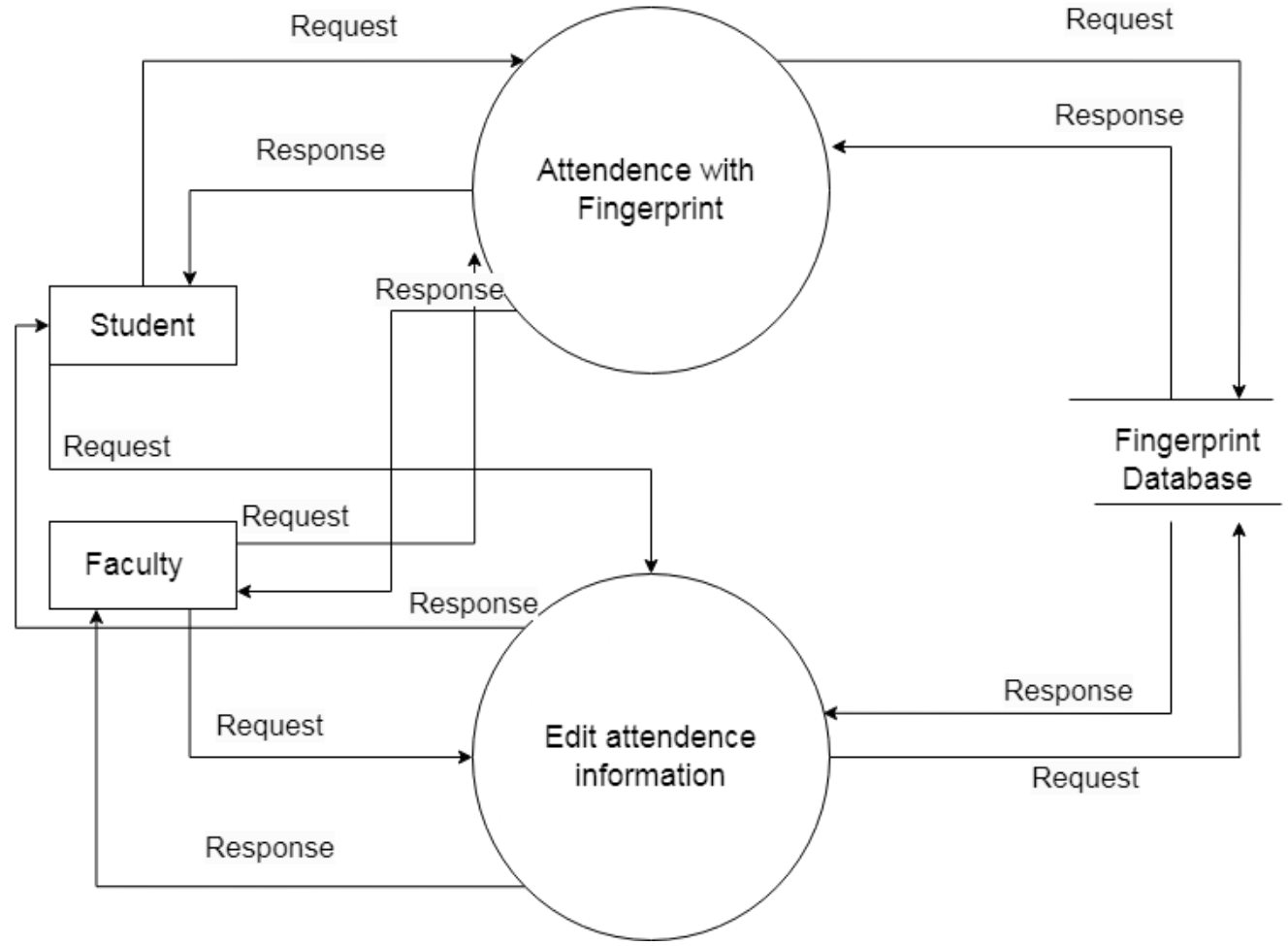
Over the course of the following pages, we will embark on an in-depth exploration of this cutting-edge solution. Our journey will take us through the manifold benefits it offers, the intricacies of its implementation, and the vast potential it holds for revolutionizing the landscape of laboratory security and management. We will traverse a landscape where the intersection of technology and education gives rise to a safer, more accountable, and effortlessly accessible laboratory environment, setting the stage for unparalleled advances in scientific discovery and academic excellence.

Chapter 3 – Design (Data Flow & Structure Flow / ER Diagram)

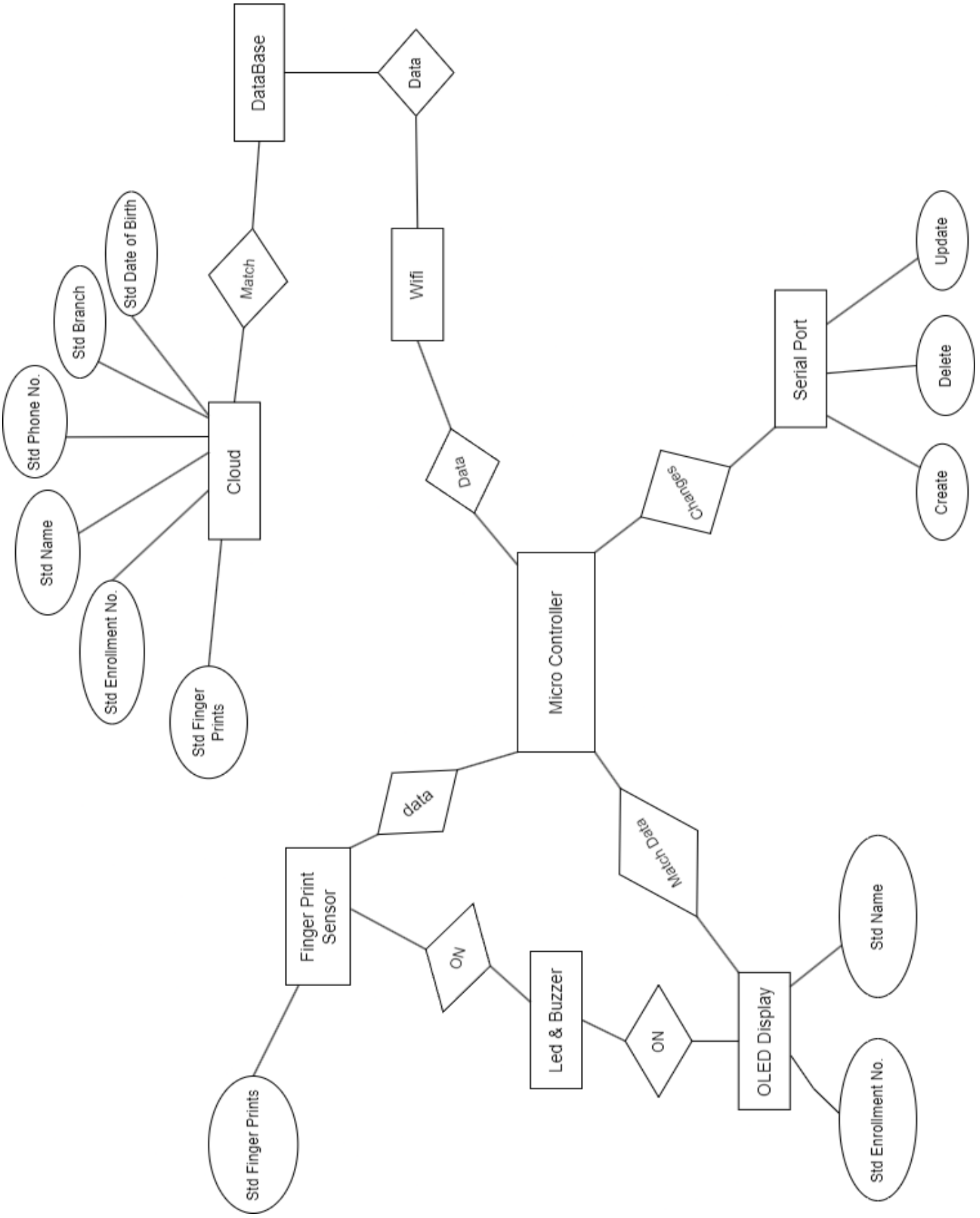
- **DFD Level 0**



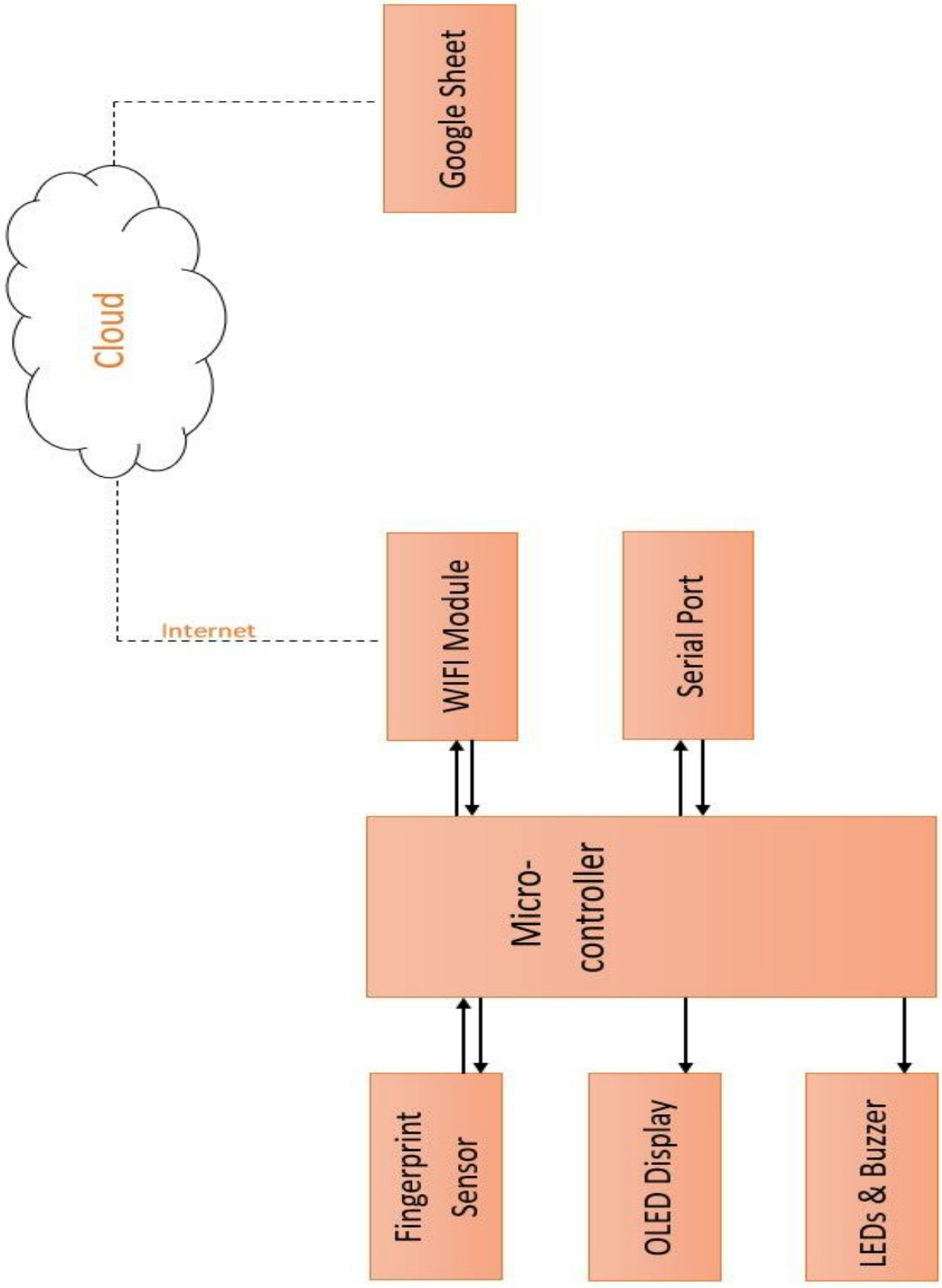
- **DFD Level 1**



- **ER Diagram**


DataBase
Data
Match
Wifi
Std Date of Birth
Std Branch
Std Phone No.
Cloud
Std Name
Std Enrollment No.
Std Finger Prints
Data
Micro Controller
Changes
Serial Port
Update
Delete
Create
data
Finger Print Sensor
ON
Led & Buzzer
ON
Match Data
OLED Display
Std Name
Std Enrollment No.
Std Finger Prints

- **Block Diagram**



Chapter 4 – Implementation Details

The successful implementation of a "Student Lab Authorization System Using Fingerprint Biometric" requires careful planning, a structured approach, and attention to various key aspects. Here are the essential implementation details in paragraphs:

1. System Infrastructure: The first step in implementing this system is to establish the necessary infrastructure. This includes the deployment of fingerprint scanning devices at laboratory entrances, as well as the installation of a secure server or cloud-based database to store and manage the biometric data and access records. The chosen infrastructure should be scalable to accommodate the institution's size and future growth.

2.Fingerprint Enrollment: Authorized students and personnel must enroll their fingerprints into the system. This process involves capturing high-resolution fingerprint images, extracting unique biometric features, and securely storing this data in the database. Enrollment stations equipped with fingerprint scanners and user-friendly interfaces should be set up to facilitate this process. During enrollment, individuals should also provide necessary identification and access permissions, which will be associated with their biometric data.

3.Biometric Data Security: Biometric data is highly sensitive and requires stringent security measures. It should be encrypted and stored securely to prevent unauthorized access or tampering. Implementing robust encryption techniques and access controls is essential to protect this sensitive information.

4.Real-time Authentication: When a student or authorized personnel attempts to access a laboratory, the system will perform real-time fingerprint authentication. The fingerprint scanner will capture the individual's fingerprint, match it against the enrolled data, and grant access if the match is successful. Access decisions should be made swiftly to ensure a seamless user experience.

5. Logging and Auditing: Comprehensive access logs should be maintained, recording all entry and exit events. These logs should include timestamped data, the identities of individuals accessing the laboratory, and the result of each authentication attempt. Auditing capabilities are essential for monitoring and investigating any security incidents or anomalies.

Chapter 5 – Hardware & Software requirements

Hardware	Specification
PC	- Hard disk 80GB Minimum - Processor 3.2 GHz Minimum. Preferable core i3 and above - RAM 4.0 GB - Graphics frequency 3.30 MHz - 64-bit Operating System
Fingerprint Scanner	- Image resolution 500 pixels per inch. - Image area 9.75mm X 0.41mm/ 192 X 8 pixel - ISO / IEC 7816 T=0 and T=1 - Up to 8Mhz smart cards, and a 412 Kbit/s communication speed

Chapter 6 – Conclusion

Conclusion:

In conclusion, the implementation of a "Student Lab Authorization System Using Fingerprint Biometric" represents a significant leap forward in addressing the challenges associated with conventional access control methods within educational institutions. This cutting-edge system offers a holistic solution that enhances security, accountability, and convenience for both students and administrative staff.

By harnessing the power of fingerprint biometrics, this system mitigates the risks associated with unauthorized access, safeguarding valuable laboratory equipment and sensitive experiments. It strengthens security measures, ensuring that only authorized individuals gain entry, while also providing real-time monitoring and comprehensive access logs for accountability and incident response.

Moreover, the user-friendly and convenient nature of the fingerprint biometric system streamlines access for authorized students, eliminating the need for physical tokens like keys or access cards. This not only enhances the overall user experience but also reduces the likelihood of lost or stolen access credentials.

As educational institutions embrace this innovative approach to laboratory access control, they not only bolster their security posture but also stay aligned with evolving technological advancements. Furthermore, the implementation of strong data security and privacy measures ensures compliance with relevant regulations.

In summary, the "Student Lab Authorization System Using Fingerprint Biometric" not only addresses the identified challenges but also paves the way for a safer, more efficient, and technologically advanced educational environment. It signifies a transformative shift towards a future where secure and convenient access to laboratory facilities becomes the norm, ultimately benefiting students, faculty, and the institution as a whole.

Chapter 7 – References

- https://jeangalea.com/best-resources-learning-electronics/
- https://www.learnabout-electronics.org/
- https://www.allaboutcircuits.com/education/
- https://www.circuitbread.com/